# Introduction to Fields

Michael Vaughan-Lee

November 2003

## 1 Introduction

Recall that a field is a commutative ring with unity, where $0 \neq 1$, and where every non-zero element has a multiplicative inverse. Thus we have the operations of $+$, $-$, $\times$, $\div$, together with constants $0, 1$, and these operations and constants satisfy the familiar rules of arithmetic we all grew up with. The most familiar examples of fields are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, but there are many other examples. In particular it turns out that there are finite fields. You should certainly be familiar with the field $\mathbb{Z}_p$, but in fact (as we will see) there are fields of order $p^n$ for every prime-power. In this course we are mainly concerned with field extensions, and finding roots of polynomials, but before we get on to this we need to investigate the notion of characteristic.

## 2 The prime subfield

Let $F$ be a field, and consider the additive subgroup generated by 1. As usual we define $2 = 1 + 1$, $3 = 2 + 1$, and so on. And, as usual, we let $-2$ be the additive inverse of 2, and so on. So the additive subgroup generated by 1 is $\{0, \pm 1, \pm 2, \ldots\}$. But beware! If $F = \mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ then this subgroup is just $\mathbb{Z}$. But if $F = \mathbb{Z}_3$ (for example) then $1 + 1 + 1 = 0$, so that $3 = 0$, $4 = 1$, $-1 = 2$ and so on. So in this case the subgroup is $\{0, 1, 2\}$, and 2 is not the integer 2 at all. In this case 0 is the set of all integers which are multiples of 3, 1 is the set of all integers which are equivalent to 1 mod 3, and 2 is the set of all integers which are equivalent to 2 mod 3. Of course this sounds like nonsense, and so to avoid confusion and nonsense we sometimes denote the zero element of $\mathbb{Z}_3$ by $\overline{0}$, the unit element by $\overline{1}$, and let $\overline{2} = \overline{1} + \overline{1}$. However the standard (quite legitimate) convention is to denote the zero element of a field by 0, and denote the unit element of a field by 1, even if these are *not* the integers 0 and 1.

But for the moment we need to be careful. So (just for the moment) let the

zero element of $F$ be $\overline{0}$, let the unit element be $\overline{1}$, let

$$\overline{n} = \underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{n}$$

for $n > 0$, and let

$$\overline{n} = \underbrace{(-\overline{1}) + (-\overline{1}) + \ldots + (-\overline{1})}_{-n}$$

for $n < 0$. (Here $-\overline{1}$ is the additive inverse of $\overline{1}$ in $F$.) Then it is easy to see that $\overline{n} + \overline{-n} = \overline{0}$, so that $\overline{-n} = -\overline{n}$, the additive inverse of $\overline{n}$. Also, if $m, n > 0$ then

$$\overline{m} + \overline{n} = \underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{m} + \underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{n} = \underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{m+n} = \overline{m+n}.$$

The proofs that $\overline{m} + \overline{n} = \overline{m+n}$ when one or other or both of $m$ and $n$ are negative are similar. Next, let $m, n > 0$ and consider $\overline{m}.\overline{n}$.

$$\overline{m}.\overline{n} = \left(\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{m}\right)\left(\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{n}\right) = \underbrace{\overline{1}^2 + \overline{1}^2 + \ldots + \overline{1}^2}_{mn} = \overline{mn}$$

since $\overline{1}^2 = \overline{1}$. Again, it is straightforward to show that $\overline{m}.\overline{n} = \overline{mn}$ for all $m, n$ (whatever their signs). (Though you have to prove that $(-\overline{1})^2 = \overline{1}$, which I leave as an exercise.)

All this shows that the map $f$ from $\mathbb{Z}$ to $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\}$ mapping $n$ to $\overline{n}$ is a ring homomorphism.

Now one of two things can happen: $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\}$ is either finite or infinite. Equivalently, the additive order of $\overline{1}$ is either finite or infinite.

**Lemma 1** *If $\overline{1}$ has finite order $n$ then $n$ is prime and $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\} \cong \mathbb{Z}_n$, and if $\overline{1}$ has infinite order then $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\} \cong \mathbb{Z}$.*

PROOF: Suppose that $\overline{1}$ has finite order $n$, and suppose that $n = rs$ (with $r, s > 0$). Then

$$\overline{r}.\overline{s} = \overline{rs} = \overline{n} = \overline{0}$$

and so since $F$ is a field either $\overline{r} = \overline{0}$ or $\overline{s} = \overline{0}$. But if $\overline{r} = \overline{0}$ then the order of $\overline{1}$ divides $r$, so that $n$ divides $r$. But this can only happen when $r = n$ and $s = 1$. Similarly, if $\overline{s} = \overline{0}$ then $r = 1$ and $s = n$. So $n$ is prime.

Now consider the homomorphism $f : \mathbb{Z} \to \{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\}$ mapping $m$ to $\overline{m}$. The integer $m$ lies in the kernel of $f$ if and only if $n$ divides $m$. So $\ker f = n\mathbb{Z}$, and $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\} = \mathrm{Im} f \cong \mathbb{Z}/\ker f = \mathbb{Z}_n$.

On the other hand, suppose that $\overline{1}$ has infinite order. Then the elements $\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots$ must all be distinct, for if $\overline{r} = \overline{s}$ for some $r > s$ then

$$\overline{r - s} = \overline{r} - \overline{s} = \overline{0}$$

and $\overline{1}$ has finite order dividing $r - s$. So if $\overline{1}$ has infinite order then the homomorphism $f$ is 1-1, and $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\} \cong \mathbb{Z}$. $\square$

Note that in the case when $\overline{1}$ has finite order $p$ ($p$ prime) then the additive subgroup generated by $\overline{1}$ is isomorphic to the field $\mathbb{Z}_p$. So $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\}$ is a field.

When $\overline{1}$ has infinite order then $\{\overline{0}, \pm\overline{1}, \pm\overline{2}, \ldots\} \cong \mathbb{Z}$, which is not a field. But if we form the set

$$K = \{\overline{r}.\overline{s}^{-1} \,|\, r, s \in \mathbb{Z},\ s \neq 0\}$$

then it is easy to see that $K$ is a subfield of $F$. Furthermore it is easy to see that the map $g : \mathbb{Q} \to K$ given by $g(r/s) = \overline{r}.\overline{s}^{-1}$ is an isomorphism.

So every field $F$ has a subfield isomorphic to $\mathbb{Q}$, or a subfield isomorphic to $\mathbb{Z}_p$ for some prime $p$. This subfield is known as the *prime subfield*, and is the unique minimal subfield of $F$. In the former case we say that $F$ has characteristic zero, and in the latter case we say that $F$ has characteristic $p$. Note that if $F$ has characteristic $p$, and if $a \in F$ then

$$\underbrace{a + a + \ldots + a}_{p} = a\left(\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{p}\right) = a.\overline{0} = \overline{0}$$

so every element has additive order $p$. And if $F$ has characteristic zero then every element has infinite order (additively), since if $a \in F$ has finite order $n$ then

$$\overline{0} = \underbrace{a + a + \ldots + a}_{n} = a\left(\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{n}\right) = a.\overline{n}$$

which implies that $a = \overline{0}$ or $\overline{n} = \overline{0}$.

From now on we will return to the standard notation of 0,1 for the zero element and unit of $F$.

# 3 The Tower Lemma

Perhaps the most important tool of all for understanding field extensions is the notion of the degree of an extension. Let $F$ and $K$ be fields, and suppose that $F \leq K$. We say that $K$ is a field extension of $F$, which is just another way of saying that $F$ is a subfield of the field $K$. We can thing of $K$ as a vector space over the field $F$. For $K$ is an abelian group under the field operations $+$, $-$, $0$, and if $v \in K$ and $\alpha \in F$ then $\alpha v \in K$ is defined by multiplication in $K$. In other words we "forget" that we actually know how to multiply elements of $K$, but we "remember" that we do know how to multiply elements of $K$ by "scalars" from

$F$. The degree of $K$ over $F$, $|K : F|$, is defined to be the dimension of $K$ when thought of as a vector space over $F$. For example, $|\mathbb{C} : \mathbb{R}| = 2$. The field $\mathbb{C}$ has a basis $1, i$ over $\mathbb{R}$, and every element of $\mathbb{C}$ can be uniquely expressed in the form $\alpha.1 + \beta i$ for two "scalars" $\alpha, \beta \in \mathbb{R}$. On the other hand $|\mathbb{R} : \mathbb{Q}|$ is infinite. We say that $K$ is a finite extension of $F$ if $|K : F|$ is finite.

**Lemma 2 (The Tower Lemma)** *Let $F \leq K \leq L$, and let $|K : F| = m$, $|L : K| = n$. Then $|L : F| = mn$.*

PROOF: Let $a_1, a_2, \ldots, a_m$ be a basis for $K$ as a vector space over $F$, and let $b_1, b_2, \ldots, b_n$ be a basis for $L$ as a vector space over $K$. We establish the lemma by proving that $\{a_i b_j \,|\, 1 \leq i \leq m,\, 1 \leq j \leq n\}$ is a basis for $L$ as a vector space over $F$.

First we show that $\{a_i b_j\}$ spans $L$ over $F$. So let $b \in L$. Then $b = \sum_{j=1}^{n} k_j b_j$ for some $k_j \in K$. And for each $j$ we have $k_j = \sum_{i=1}^{m} f_{ij} a_i$ for some $f_{ij} \in F$. So $b = \sum_{i,j} f_{ij} a_i b_j$.

And now we show that $\{a_i b_j\}$ is linearly independent. Suppose that $\sum_{i,j} f_{ij} a_i b_j = 0$. Then

$$\sum_{j=1}^{n} \left( \sum_{i=1}^{m} f_{ij} a_i \right) b_j = 0.$$

Now for each $j$, $\sum_{i=1}^{m} f_{ij} a_i \in K$, and $b_1, b_2, \ldots, b_n$ are linearly independent over $K$. So $\sum_{i=1}^{m} f_{ij} a_i = 0$ for all $j = 1, 2, \ldots, n$. But $a_1, a_2, \ldots, a_m$ are linearly independent over $F$, and so $\sum_{i=1}^{m} f_{ij} a_i = 0$ implies that $f_{ij} = 0$ for all $i$. Hence $f_{ij} = 0$ for all $i, j$, and we are done. □

# 4 Simple extensions

Let $K$ be a field extension of the field $F$, and let $a \in K$. We let $F(a)$ be the smallest subfield of $K$ which contains both $F$ and $a$. We say that $F(a)$ is a *simple extension* of $F$. Understanding simple extensions is the key to understanding the "Introduction to Fields" syllabus.

Subfields are closed under multiplication, and so since $F(a)$ contains $a$, $F(a)$ also contains $a^2, a^3, \ldots$. Also $F(a)$ contains 1 (since it is a subfield), and so $1, a, a^2, \ldots \in F(a)$. Closing this set under addition and under multiplication by elements of $F$ we see that

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_k a^k \in F(a)$$

for all $\alpha_0, \alpha_1, \ldots, \alpha_k \in F$ and all $k \geq 0$. In other words $f(a) \in F(a)$ for all polynomials

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k \in F[x].$$

The set $\{f(a) \mid f(x) \in F[x]\}$ is denoted $F[a]$. So $F[a]$ is the set of all polynomials in $a$ with coefficients from $F$, and $F[a]$ is contained in the subfield $F(a)$. The situation we are interested in is when $F[a]$ is closed under division, so that $F[a]$ is a field and $F[a] = F(a)$. But in general $F[a]$ is not closed under division and

$$F(a) = \{f(a).g(a)^{-1} \mid f(x), g(x) \in F[x],\ g(a) \neq 0\}.$$

(Clearly the set $\{f(a).g(a)^{-1}\}$ above is closed under $+$, $-$, $\times$, $\div$ and contains 0,1 and so it is a subfield of $K$. Equally clearly any subfield of $K$ containing both $F$ and $a$ must contain all the elements $f(a).g(a)^{-1}$.)

**Definition 3** *We say that $a$ is* algebraic *over $F$ if $f(a) = 0$ for some non-zero polynomial $f(x) \in F[x]$. If $a$ is not algebraic over $F$ then we say that $a$ is* transcendental *over $F$.*

We will show that $F[a]$ is a subfield of $K$ (so that $F(a) = F[a]$) if and only if $a$ is algebraic over $F$.

**Lemma 4** *The element $a$ is algebraic over $F$ if and only if $1, a, a^2, \ldots$ are linearly dependent over $F$.*

PROOF: Note that we say that an infinite set is linearly independent if every finite subset is linearly independent. Conversely, an infinite set is linearly dependent if some finite subset is linearly dependent.

Suppose that $a$ is algebraic over $F$. Then $f(a) = 0$ for some non-zero polynomial $f(x) \in F[x]$ and so

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_k a^k = 0$$

for some $\alpha_0, \alpha_1, \ldots, \alpha_k \in F$, not all of which are zero. So $1, a, a^2, \ldots, a^k$ are linearly dependent.

On the other hand suppose that $1, a, a^2, \ldots, a^k$ are linearly dependent. Then

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_k a^k = 0$$

for some $\alpha_i$ which are not all zero. Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k$. Then $f(a) = 0$ and so $a$ is algebraic over $F$. □

**Definition 5** *If $a$ is algebraic over $F$ then the minimal polynomial of $a$ is the monic polynomial $m(x)$ of least degree such that $m(a) = 0$.*

**Lemma 6** *If $a$ is algebraic over $F$ then*

1. *the minimal polynomial $m(x)$ of $a$ is unique,*

2. *$f(a) = 0$ if and only if $m(x)|f(x)$,*

3. *$m(x)$ is irreducible.*

PROOF: We prove (2) first. Clearly, if $m(x)|f(x)$ then $f(a) = 0$. Conversely suppose that $f(a) = 0$. By the division algorithm for polynomials over a field, there are polynomials $q(x), r(x)$ with $\deg r < \deg m$ such that $f(x) = m(x)q(x) + r(x)$. Thus

$$0 = f(a) = m(a)q(a) + r(a) = r(a).$$

By the choice of $m(x)$ this implies that $r(x) = 0$, and so $m(x)|f(x)$.

(2) implies (1) since if $m_1(x)$ and $m_2(x)$ are two minimal polynomials then $m_1|m_2$ and $m_2|m_1$. Since they are both monic this implies that $m_1 = m_2$.

To establish (3) let $m(x) = r(x)s(x)$ where $\deg r, \deg s < \deg m$. Then $r(a)s(a) = m(a) = 0$ and so either $r(a) = 0$ or $s(a) = 0$. But this is impossible by the definition of $m(x)$. So $m(x)$ is irreducible. □

**Theorem 7** *If $F$ and $K$ are fields with $F \leq K$ and if $a \in K$ is algebraic over $F$ with minimal polynomial $m(x)$ of degree $n$ then*

1. *$F(a) = F[a] \cong F[x]/I$ where $I = m(x)F[x]$,*

2. *$|F[a] : F| = n$, and $F[a]$ has basis $1, a, a^2, \ldots, a^{n-1}$ as a vector space over $F$.*

PROOF: As we observed above, $F[a]$ is a commutative ring with unity containing $F$ and $a$. To show that $F[a]$ is a field we have to show that it is closed under division. So let $f(x) \in F[x]$ and suppose that $f(a) \neq 0$. Then $m(x) \nmid f(x)$ and so (since $m(x)$ is irreducible) $\gcd(m(x), f(x)) = 1$. So there are polynomials $r(x), s(x)$ such that $m(x)r(x) + f(x)s(x) = 1$. This gives

$$1 = m(a)r(a) + f(a)s(a) = f(a)r(a)$$

and so $f(a)^{-1} = r(a) \in F[a]$. So $F[a]$ is a field.

We define a map $\pi : F[x] \to F[a]$ by setting $\pi(f(x)) = f(a)$. Clearly $\pi$ is homomorphism and $\ker \pi = m(x)F[x] = I$. So

$$F[a] = \mathrm{Im}\pi \cong F[x]/\ker \pi = F[x]/I.$$

(Note that since $m(x)$ is irreducible, $I$ is a maximal ideal of $F[x]$ which implies that $F[x]/I$ is a field. Since $F[a] \cong F[x]/I$ this gives an alternative proof of the fact that $F[a]$ is a field.)

Since the minimal polynomial of $a$ has degree $n$, it follows that $1, a, a^2, \ldots, a^{n-1}$ are linearly independent. We show that they span $F[a]$, and to do this we

need to show that $a^k \in Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle$ for all $k \geq 0$. Clearly $a^k \in Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle$ for $k = 0, 1, \ldots, n-1$. And if we let

$$m(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} + x^n$$

then

$$a^n = -\alpha_0 - \alpha_1 a - \ldots - \alpha_{n-1}a^{n-1} \in Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle.$$

Suppose by induction that $a^k \in Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle$ for $0 \leq k \leq m$ for some $m \geq n$. So

$$a^m = \beta_0 + \beta_1 a + \ldots + \beta_{n-1}a^{n-1}$$

for some $\beta_i$. Then

$$a^{m+1} = \beta_0 a + \beta_1 a^2 + \ldots + \beta_{n-1}a^n \in Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle$$

since $a, a^2, \ldots, a^n$ all lie in $Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle$. So $F[a] = Sp\langle 1, a, a^2, \ldots, a^{n-1}\rangle$.

Hence $1, a, a^2, \ldots, a^{n-1}$ is a basis for $F[a]$ over $F$, and $|F(a) : F| = n = \deg m$. □

**Example 8** *The element $2^{1/3}$ satisfies the polynomial $x^3 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. So $x^3 - 2$ is the minimal polynomial of $2^{1/3}$ over $\mathbb{Q}$. It follows that $\mathbb{Q}[2^{1/3}]$ is a field with basis $1, 2^{1/3}, 2^{2/3}$ over $\mathbb{Q}$.*

**Example 9** *The element $\omega = e^{2\pi i/3}$ is a complex cube root of unity, and so satisfies the polynomial $x^3 - 1$. But $x^3 - 1 = (x-1)(x^2 + x + 1)$, and so the minimal polynomial of $\omega$ over $\mathbb{Q}$ is $x^2 + x + 1$. So $\mathbb{Q}[\omega]$ is a field with basis $1, \omega$ over $\mathbb{Q}$.*

**Theorem 10** *If $F$ and $K$ are fields with $F \leq K$ and if $a \in K$ is transcendental over $F$ then*

1. $F(a) \cong F(x) = \{f(x)/g(x) \mid f(x), g(x) \in F[x],\ g(x) \neq 0\}$,
2. $|F(a) : F| = \infty$.

PROOF: Since $a$ is transcendental over $F$ the elements $1, a, a^2, \ldots$ are linearly independent over $F$ and $F(a)$ cannot be finite dimensional over $F$. So $|F(a) : F| = \infty$. As we showed above

$$F(a) = \{f(a).g(a)^{-1} \mid f(x), g(x) \in F[x],\ g(a) \neq 0\}.$$

We establish (1) by showing that $f(a).g(a)^{-1} = r(a).s(a)^{-1}$ if and only if $f(x)/g(x) = r(x)/s(x)$.

So suppose that $f(a).g(a)^{-1} = r(a).s(a)^{-1}$. Multiplying both sides of this equation by $g(a)s(a)$ we obtain $f(a).s(a) = r(a).g(a)$. So $a$ satisfies the polynomial $f(x)s(x) - r(x)g(x)$. Since $a$ is transcendental this implies that $f(x)s(x) - r(x)g(x) = 0$ and hence that $f(x)/g(x) = r(x)/s(x)$.

Clearly if $f(x)/g(x) = r(x)/s(x)$ then $f(a).g(a)^{-1} = r(a).s(a)^{-1}$, and so the correspondence

$$f(a).g(a)^{-1} \leftrightarrow f(x)/g(x)$$

gives an isomorphism between $F(a)$ and $F(x)$. □

Note that in some sense this means that all transcendental elements look alike! The real numbers e and $\pi$ are transcendental over $\mathbb{Q}$. There is a proof in Chapter 5 of Herstein, though it is not all that easy.

Note also that the two theorems above give another characterization of the property of being algebraic.

**Theorem 11** *Let $F$ and $K$ be fields, and let $F \leq K$. If $a \in K$ then $a$ is algebraic over $F$ if and only if $F(a)$ is a finite extension of $F$.*

PROOF: As we showed above, if $a$ is algebraic then $|F(a) : F|$ is finite. But conversely, if $|F(a) : F| = n$ then $1, a, a^2, \ldots, a^n$ are $n + 1$ elements (vectors) in an $n$-dimensional space, and so they must be linearly dependent. So $a$ satisfies a non-zero polynomial of degree at most $n$, and $a$ is algebraic. □

**Lemma 12** *If $a, b$ are both algebraic over $F$ (with $b \neq 0$), then so are $a \pm b$, $ab$, $a.b^{-1}$.*

PROOF: Let the minimal polynomials of $a$ and $b$ have degrees $m$ and $n$ respectively. Then $|F(a) : F| = m$. Consider the field $(F(a))(b) = F(a, b)$. The element $b$ satisfies a polynomial of degree $n$ with coefficients in $F$. These coefficients lie in $F(a)$ and so $b$ is algebraic over $F(a)$. Furthermore the minimal polynomial of $b$ over $F(a)$ has degree at most $n$. (The degree can be less than $n$. For example we could have $b \in F(a)$ so that $b$ satisfies the polynomial $x - b$ over $F(a)$.) So $|F(a, b) : F(a)| \leq n$ and by the Tower Lemma

$$|F(a, b) : F| = |F(a, b) : F(a)| \cdot |F(a) : F| \leq mn.$$

Now consider $a + b$. Clearly $a + b \in F(a, b)$ and so $F \leq F(a + b) \leq F(a, b)$. This implies that $|F(a + b) : F| \leq mn$, and hence that $a + b$ is algebraic over $F$. Similarly $a-b$, $ab$, and $a.b^{-1} \in F(a, b)$ and so they also are algebraic over $F$. □

**Definition 13** *Let $F$ and $K$ be fields, and let $F \leq K$. We say that $K$ is an algebraic extension of $F$ if every element of $K$ is algebraic over $F$.*

Note that $K$ can be an infinite extension of $F$ and still be algebraic over $F$. Consider the subset $A$ of the complex numbers consisting of all elements $a \in \mathbb{C}$ such that $a$ is algebraic over $\mathbb{Q}$. Then the lemma above implies that $A$ is a subfield of $\mathbb{C}$, and clearly $A$ is algebraic over $\mathbb{Q}$. But $A$ contains roots of the irreducible polynomial $x^n - 2$ for all $n \geq 2$ (for example). If $a$ is one of these roots then the minimal polynomial of $a$ is $x^n - 2$ so that

$$\mathbb{Q} \leq F(a) \leq A$$

where $|F(a) : \mathbb{Q}| = n$. Thus $|A : \mathbb{Q}| \geq n$ for all $n \geq 2$.

**Theorem 14** *If $F, K, L$ are fields, and if $K$ is an algebraic extension of $F$, and $L$ is an algebraic extension of $K$, then $L$ is an algebraic extension of $F$.*

PROOF: Let $a \in L$. Then $a$ is algebraic over $K$ and so $f(a) = 0$ for some non-zero polynomial

$$k_0 + k_1 x + \ldots + k_n x^n \in K[x].$$

For each $i = 0, 1, \ldots, n$ the coefficient $k_i$ is algebraic over $F$ and so satisfies a polynomial $p_i(x) \in F[x]$. Let $\deg p_i = m_i$. Consider the field $F(k_0, k_1, \ldots, k_n)$. We have $|F(k_0) : F| \leq m_0$. And since $k_1$ satisfies a polynomial of degree $m_1$ with coefficients in $F$ we have $|F(k_0, k_1) : F(k_0)| \leq m_1$. The Tower Lemma then gives $|F(k_0, k_1) : F| \leq m_0 m_1$. Continuing in this way we see that $|F(k_0, k_1, \ldots, k_n) : F| \leq m_0 m_1 \ldots m_n$. And since $a$ satisfies a polynomial of degree $n$ over $F(k_0, k_1, \ldots, k_n)$ we have

$$|F(k_0, k_1, \ldots, k_n, a) : F| \leq m_0 m_1 \ldots m_n n.$$

This implies that $|F(a) : F| \leq m_0 m_1 \ldots m_n n$, so that $a$ is algebraic over $F$. $\square$

# 5 Roots of polynomials

The theorem above showing that if $a$ is algebraic over $F$ with minimal polynomial $m(x)$ then $F(a) \cong F[x]/I$ where $I$ is the ideal $m(x)F[x]$ can be stood on its head to construct new fields with our bare hands.

Let $F$ be a field, and let $m(x)$ be an irreducible polynomial in $F[x]$. Consider the ideal $I = m(x)F[x]$. This is a maximal ideal of $F[x]$, which is a commutative ring with unity. So $F[x]/I$ is a field. (To see that $I$ is maximal recall that $F[x]$ is a principal ideal domain, so that if $I \leq J \lhd F[x]$ then $J = p(x)F[x]$ for some polynomial $p(x)$. Since $m(x) \in I \leq J$ we have $p(x)|m(x)$. But $m(x)$ is irreducible

and so either $p(x)$ is a constant polynomial and $J = F[x]$, or $p(x)$ is a constant multiple of $m(x)$ and $J = I$.)

The elements of $F[x]/I$ are of the form $f(x) + I$, with $f(x) \in F[x]$. We can write $f(x) = m(x)q(x) + r(x)$ for some $q(x), r(x)$, where $\deg r < \deg m$. Since $f(x) - r(x) \in I$ we see that $f(x) + I = r(x) + I$. So if $\deg m = n$ then every element of $F[x]/I$ can be expressed in the form

$$\alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} + I.$$

We identify $F$ with the subfield of $F[x]/I$ consisting of elements $\alpha + I$ ($\alpha \in F$). So $F[x]/I$ is an extension field of $F$ and $F[x]/I$ is spanned over $F$ by the elements $1 + I, x + I, x^2 + I, \ldots, x^{n-1} + I$. Furthermore these $n$ spanning elements are linearly independent over $F$ for if $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in F$ then

$$\alpha_0(1 + I) + \alpha_1(x + I) + \ldots + \alpha_{n-1}(x^{n-1} + I) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} + I$$

and if this equals zero then $\alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} \in I$, which can only arise when $\alpha_0 = \alpha_1 \ldots = \alpha_{n-1} = 0$. Hence $F[x]/I$ has the elements $1 + I, x + I, x^2 + I, \ldots, x^{n-1} + I$ as a basis over $F$.

So $|F[x]/I : F| = n$. If we let $a = x + I \in F[x]/I$ then $a^2 = (x + I)(x + I) = x^2 + I$, $a^3 = x^3 + I$, and so on. As above we identify $1 + I$ with $1 \in F$, so that $F[x]/I$ has a basis $1, a, a^2, \ldots, a^{n-1}$ as a vector space over $F$. Thus $F[x]/I = F[a]$. Furthermore

$$m(a) = m(x + I) = m(x) + I = 0 + I$$

since $m(x) \in I$. So $a$ is a root of the polynomial $m(x)$ that we started with.

To summarize, if $F$ is a field and if $m(x)$ is an irreducible polynomial in $F[x]$, then we can construct a field extension $K$ of $F$ where $|K : F| = n$, and where $K$ contains an element $a$ such that $a$ is root of $m(x)$ and such that $K = F[a]$.

An important example is $\mathbb{C} = \mathbb{R}[i]$. The minimal polynomial of $i$ over $\mathbb{R}$ is $x^2 + 1$. So $\mathbb{C} = \mathbb{R}[x]/Id\langle x^2 + 1\rangle$. In many ways this is a much better way of defining $\mathbb{C}$ than the usual way which is as the set of ordered pairs of real numbers with a rather twisted multiplication. Although the definition of the quotient ring $\mathbb{R}[x]/Id\langle x^2 + 1\rangle$ is somewhat sophisticated, it ultimately comes down to something very easy — take the set of polynomials in $\mathbb{R}[x]$, and then set $x^2 + 1 = 0$ (equivalently set $x^2 = -1$). You need the sophistication to know that this really works, but you don't need the sophistication to apply it.

# 6 Splitting fields

Let $F$ and $K$ be fields, and let $f(x) \in F[x]$. Then we say that $f(x)$ splits in $K$ if $f(x)$ can be factorized into a product of linear factors

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

with $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, for some constant $a \in F$. (Usually we only consider monic polynomials, and then $a = 1$.) The splitting field for $f(x)$ over $F$ in $K$ is then $F[\alpha_1, \alpha_2, \ldots, \alpha_n]$. (Note that this is an algebraic extension of $F$ since $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all roots of the polynomial $f(x)$.) We say that $K$ is a splitting field for $f(x)$ if $K = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$. In other words $K$ is a splitting field for $f(x)$ over $F$ if $f(x)$ splits into a product of linear factors over $K$, and if $K$ is generated over $F$ by the roots of $f(x)$. We will show that for every field $F$ and for every polynomial $f(x) \in F[x]$ we can construct a splitting field for $f(x)$ over $F$. It turns out that any two such splitting fields are isomorphic (though the details of the proof of this are outside the "Introduction to Fields" syllabus), and so we often refer to "the splitting field", rather than to "a splitting field".

For example $\mathbb{C}$ is the splitting field for $x^2 + 1$ over $\mathbb{R}$.

The fundamental theorem of algebra states that any polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$. So if (for example) $f(x) \in \mathbb{Q}[x]$, and we want to find the splitting field for $f(x)$ over $\mathbb{Q}$, then we can find the roots of $f(x)$ in $\mathbb{C}$, and the splitting field is the subfield of $\mathbb{C}$ generated over $\mathbb{Q}$ by the roots. For example consider the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. This is irreducible over $\mathbb{Q}$ by Eisenstein's criterion, but over $\mathbb{C}$

$$x^3 - 2 = (x - 2^{1/3})(x - \omega 2^{1/3})(x - \omega^2 2^{1/3})$$

where $\omega = \mathrm{e}^{2\pi i/3}$. So the splitting field is

$$\mathbb{Q}[2^{1/3}, \omega 2^{1/3}, \omega^2 2^{1/3}].$$

This field is usually written as $\mathbb{Q}[2^{1/3}, \omega]$ since any field which contains $2^{1/3}$, $\omega 2^{1/3}$ and $\omega^2 2^{1/3}$ also contains $2^{1/3}$ and $\omega$, and vice-versa. We can work out the degree of the splitting field over $\mathbb{Q}$ as follows. We have

$$\mathbb{Q} \leq \mathbb{Q}[2^{1/3}] \leq \mathbb{Q}[2^{1/3}, \omega].$$

The minimal polynomial of $2^{1/3}$ over $Q$ is $x^3 - 2$ (since this is irreducible by Eisenstein's criterion). So $|\mathbb{Q}[2^{1/3}] : \mathbb{Q}| = 3$. The minimal polynomial of $\omega$ over $\mathbb{Q}$ is $x^2 + x + 1$, but to compute $|\mathbb{Q}[2^{1/3}, \omega] : \mathbb{Q}[2^{1/3}]|$ we need to know the minimal polynomial of $\omega$ over $\mathbb{Q}[2^{1/3}]$, which might conceivably be of lower degree. In general this is quite a tricky issue, but in this case it is straightforward. We know that $\omega \notin \mathbb{Q}[2^{1/3}]$ since $\omega$ is complex and $\mathbb{Q}[2^{1/3}]$ is real. So the minimal polynomial of $\omega$ over $\mathbb{Q}[2^{1/3}]$ must be of degree at least 2. But the minimal polynomial divides $x^2 + x + 1$ so it is of degree at most 2. Hence the degree is exactly 2, and $|\mathbb{Q}[2^{1/3}, \omega] : \mathbb{Q}[2^{1/3}]| = 2$. By the Tower Lemma $|\mathbb{Q}[2^{1/3}, \omega] : \mathbb{Q}| = 6$. In addition the proof of the Tower Lemma gives us a basis for $\mathbb{Q}[2^{1/3}, \omega]$ over $\mathbb{Q}$. We know that $\mathbb{Q}[2^{1/3}]$ has basis $1, 2^{1/3}, 2^{2/3}$ over $\mathbb{Q}$, and we know that $\mathbb{Q}[2^{1/3}, \omega]$ has basis $1, \omega$ over $\mathbb{Q}[2^{1/3}]$. So $\mathbb{Q}[2^{1/3}, \omega]$ has basis 1, $2^{1/3}$, $2^{2/3}$, $\omega$, $\omega 2^{1/3}$, $\omega 2^{2/3}$ over $\mathbb{Q}$.

**Theorem 15** *Let $F$ be a field and let $f(x) \in F[x]$ be a polynomial of degree $n$. Then we can construct a splitting field $K$ for $f(x)$ over $F$, and $|K : F| \leq n!$.*

PROOF: The proof is by induction on $n$, and relies heavily on the fact that if $m(x) \in F[x]$ is a irreducible then we can construct an extension field of $F$ in which $m(x)$ has a root.

The case $n = 1$ is trivial since if $f(x)$ has degree 1 then $f(x)$ splits in $F$ and we can take $K = F$. So we suppose that the result is true for polynomials of degree less than $n$, and we let $f(x) \in F[x]$ have degree $n$.

Let $m(x) \in F[x]$ be an irreducible factor of $f(x)$, and let $F_1 = F[x]/Id(m(x))$. Then, as we showed above, $F_1 = F[a]$ for some $a$ such that $m(a) = 0$. Furthermore $|F_1 : F| = \deg m \leq n$. Since $m(x)|f(x)$ it follows that $f(a) = 0$, and so

$$f(x) = (x - a)g(x)$$

for some $g(x) \in F_1[x]$ of degree $n - 1$. By induction we can construct a splitting field $K$ for $g(x)$ over $F_1$ with $|K : F_1| \leq (n - 1)!$. Then $K$ is a splitting field for $f(x)$ over $F$ and

$$|K : F| = |K : F_1| \cdot |F_1 : F| \leq (n - 1)!.n = n!.$$

□

With a little more care we can do slightly better than this.

**Theorem 16** *Let $F$ be a field and let $f(x) \in F[x]$ be a polynomial of degree $n$. Then we can construct a splitting field $K$ for $f(x)$ over $F$, and $|K : F|$ divides $n!$.*

PROOF: As above we proceed by induction on $n$. If $f(x)$ is irreducible we let $F_1 = F[x]/Id(f(x))$. As above, $F_1 = F[a]$ for some $a$ such that $f(a) = 0$. But now $|F_1 : F| = \deg f = n$. As above

$$f(x) = (x - a)g(x)$$

for some $g(x) \in F_1[x]$ of degree $n - 1$. By induction we can construct a splitting field $K$ for $g(x)$ over $F_1$ with $|K : F_1|$ *dividing* $(n - 1)!$. Then $K$ is a splitting field for $f(x)$ over $F$ and

$$|K : F| = |K : F_1| \cdot |F_1 : F| \text{ which divides } n!.$$

But what do we do when $f(x)$ is not irreducible? Let $f(x) = g(x)h(x)$ where $g(x), h(x) \in F[x]$ have degrees $r, s$ respectively (with $r, s \geq 1$). Let $L$ be a splitting field for $g(x)$ over $F$, and let $K$ be splitting field for $h(x)$ over $L$. Then by induction $|L : F|$ divides $r!$, and $|K : L|$ divides $s!$. Clearly $K$ is a splitting field for $f(x)$ over $F$, and $|K : F| = |K : L| \cdot |L : F|$, which divides $r!.s!$. Now for the cunning bit! We have $r + s = \deg f = n$ and the binomial coefficient

${}_nC_r = n!/(r!.s!)$ is an integer. So $r!.s!$ divides $n!$, and we are done. $\square$

In general it is quite hard to actually compute splitting fields in practice. But there is one particular special case which is quite straightforward, and often comes up in Finals. (It often comes up precisely because it is straightforward.) This special case is computing the splitting field of a polynomial of the form $x^n - 1$ over $\mathbb{Q}$. We know that the roots of this polynomial in $\mathbb{C}$ are $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ where $\zeta = \mathrm{e}^{2\pi i/n}$. So the splitting field is $\mathbb{Q}[\zeta]$. And for any given $n$ it is quite easy to factorize $x^n - 1$ and find the minimal polynomial of $\zeta$ over $\mathbb{Q}$. For example take $n = 12$.

$$x^{12} - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1).$$

The different powers of $\zeta$ are roots of the different factors: 1 is a root of $x-1$, $\zeta^6$ is a root of $x+1$, $\zeta^4$ and $\zeta^8$ are cube roots of unity so they are roots of $x^2+x+1$, $\zeta^2$ and $\zeta^{10}$ are sixth roots of unity so they are roots of $x^2 - x + 1$, $\zeta^3$ and $\zeta^9$ are fourth roots of unity and are roots of $x^2 + 1$. This leaves the four primitive 12-th roots of unity $\zeta, \zeta^5, \zeta^7$ and $\zeta^{11}$ and these must all be roots of $x^4 - x^2 + 1$. (We call them primitive 12-th roots since they are not roots of $x^n - 1$ for any $n < 12$, whereas all the other roots of $x^{12} - 1$ are roots of $x^n - 1$ for some $n < 12$.) Thus the minimal polynomial of $\zeta$ over $\mathbb{Q}$ has degree 4 and the splitting field $\mathbb{Q}[\zeta]$ has degree 4 over $\mathbb{Q}$.

The primitive $n$-th roots of unity are the numbers $\mathrm{e}^{2k\pi i/n}$ where $1 \leq k < n$ and where $k$ is relatively prime to $n$. (If $\gcd(k,n) = d > 1$, and if we write $k = rd$, $n = md$, then $\mathrm{e}^{2k\pi i/n} = \mathrm{e}^{2r\pi i/m}$ which is an $m$-th root of unity.) So the number of primitive $n$-th roots of unity is $\varphi(n) = |\{k \,|\, 1 \leq k < n, \gcd(k,n) = 1\}|$. It turns out that all the primitive $n$-th roots have the same minimal polynomial, which thus always has degree $\varphi(n)$. However this is quite tricky to prove and both the proof and the result are outside the syllabus. Nevertheless it is useful to know the answer before you start. It is easy to see that $\varphi(12) = 4$ and so in factorizing $x^{12} - 1$ you look for an irreducible factor of degree 4.

Let us look at one further example: $x^9 - 1$. If we let $\zeta = \mathrm{e}^{2\pi i/9}$ then the primitive 9-th roots of unity are $\zeta^k$ for $k = 1, 2, 4, 5, 7, 8$. So we expect the minimal polynomial of $\zeta$ to have degree 6. Now start factorizing $x^9 - 1$.

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) = (x-1)(x^2+x+1)(x^6+x^3+1).$$

Since $\varphi(9) = 6$ we "expect" $x^6 + x^3 + 1$ to be irreducible. And of course it is irreducible, though you still have to prove that it is. The point is that you won't waste any time trying to factorize it.

# 7 Finite fields

Let $F$ be a finite field. As we showed above, every field contains a subfield isomorphic to $\mathbb{Q}$ or a subfield isomorphic to $\mathbb{Z}_p$ for some prime $p$. Since $F$ is finite it must have a subfield isomorphic to $\mathbb{Z}_p$. So $F$ has finite characteristic $p$, and $F$ is an extension field of $\mathbb{Z}_p$. Since $F$ is finite it has a finite spanning set as a vector space over $\mathbb{Z}_p$ and so it is finite dimensional over $\mathbb{Z}_p$. Let $|F : \mathbb{Z}_p| = n$. If we pick a basis $v_1, v_2, \ldots, v_n$ for $F$ as a vector space over $\mathbb{Z}_p$ then every element of $F$ can be expressed uniquely in the form $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$ with $\alpha_i \in \mathbb{Z}_p$. There are $p$ choices for each coefficient $\alpha_i$ and so $F$ has $p^n$ elements. To summarize, if $F$ is a finite field then $|F| = p^n$ for some prime $p$ and some integer $n \geq 1$, and $F$ has characteristic $p$ and is an extension field of $\mathbb{Z}_p$.

The non-zero elements of $F$ form a group under multiplication (this is true in any field), and the order of this group is $p^n - 1$. By Lagrange's Theorem, if $a \in F \backslash \{0\}$ then $a^{p^n-1} = 1$. So $a^{p^n} = a$. Clearly $0^{p^n} = 0$ and so *every* element of $F$ is a root of the polynomial $x^{p^n} - x$. Now a polynomial of degree $p^n$ can have at most $p^n$ roots, and we have just shown that all $p^n$ elements of $F$ are roots of $x^{p^n} - x$. So $x^{p^n} - x$ splits in $F$, and $F$ is the splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$.

We can turn this analysis around to construct fields of order $p^n$ for all $p$ and $n$. Let $F$ be the splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$. So

$$x^{p^n} - x = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{p^n})$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_{p^n} \in F$, and $F$ is generated by these roots over $\mathbb{Z}_p$.

The first thing to note is that these roots are all distinct. If a polynomial has a repeated root then it has a factor in common with its formal derivative. But the formal derivative of $x^{p^n} - x$ is $p^n x^{p^n-1} - 1$ which as no roots in $F$ since $F$ has characteristic $p$ so that $p^n a^{p^n-1} - 1 = -1$ for all $a \in F$. So $x^{p^n} - x$ has no roots in common with its formal derivative, and so has no repeated roots.

The next thing to note is that the set of roots form a subfield of $F$ containing $\mathbb{Z}_p$. If $a \in \mathbb{Z}_p$ then $a^p = a$ (using Lagrange's Theorem as above). So

$$a^{p^n} = (\ldots((a^p)^p)\ldots)^p = a,$$

and $a$ is a root. And if $a, b$ are roots then $(a + b)^{p^n} = a^{p^n} + b^{p^n} = a + b$ (since all the binomial coefficients of the cross terms are divisible by $p$). So $a + b$ is a root. Similarly $-a$, $ab$, and $a^{-1}$ (if $a \neq 0$) are roots. So the set $\{\alpha_1, \alpha_2, \ldots, \alpha_{p^n}\}$ of roots contains $\mathbb{Z}_p$ and is closed under $+$, $-$, $\times$, and $\div$. This implies that the set of roots *is* the splitting field $F$. And since there are $p^n$ roots $|F| = p^n$.

Thus we have shown that every finite field has order $p^n$ for some $p$ and $n$, and we have shown that there is a unique finite field of order $p^n$ for every $p$ and every $n$. (The uniqueness comes from the uniqueness of the splitting field.)

For example the field $GF(4)$ of four elements is the splitting field of $x^4 - x$ over $\mathbb{Z}_2$. Now

$$x^4 - x = x(x - 1)(x^2 + x + 1)$$

and if we let $\omega$ be a root of $x^2+x+1$ in $GF(4)$ then $GF(4)=\{0,1,\omega,\omega^2\}$. The multiplication table of $GF(4)$ follows trivially from the fact that $\omega^3=1$. And if we use the fact that $1+\omega+\omega^2=0$, and use the fact that $GF(4)$ has characteristic 2 (so that $a+a=0$ for all $a\in GF(4)$), then the addition table is also easy to compute:

$$\begin{aligned} 1+\omega &= \omega+1=\omega^2, \\ 1+\omega^2 &= \omega^2+1=\omega, \\ \omega+\omega^2 &= \omega^2+\omega=1. \end{aligned}$$

## 7.1 Subfields

Consider the case when $F$ is a finite field, and $K$ is a subfield of $F$. Clearly $K$ must have the same characteristic as $F$ and so we have

$$\mathbb{Z}_p \leq K \leq F$$

for some prime $p$. And we must have $|F|=p^n$, $|K|=p^m$ for some $m,n$. If $|F:K|=k$ then $|F|=|K|^k$ and so $p^n=p^{mk}$ and $m|n$. So we have shown that if $K$ is a subfield of the finite field $F$ where $|F|=p^n$ then $|K|=p^m$ for some $m|n$. The converse is also true. If $F$ is a field of order $p^n$ and if $m$ divides $n$ then $F$ has a unique subfield of order $p^m$. To see this let $F$ be a finite field of order $p^n$, let $m|n$, and let $L$ be the splitting field of the polynomial $x^{p^m}-x$ over $F$. Let $a$ be any root of $x^{p^m}-x$ in $L$. Then $a^{p^m}=a$ which implies that

$$\begin{aligned} a^{p^{2m}} &= (a^{p^m})^{p^m}=a^{p^m}=a, \\ a^{p^{3m}} &= (a^{p^{2m}})^{p^m}=a^{p^m}=a, \end{aligned}$$

and so on. So $a$ is a root of $x^{p^{km}}-x$ for all $k$ and since $m|n$ we see that $a$ is a root of $x^{p^n}-x$. But $F$ is the splitting field for the polynomial $x^{p^n}-x$ over $\mathbb{Z}_p$ and so every root of $x^{p^n}-x$ in $L$ must lie in $F$. So $L$ is generated over $F$ by roots of $x^{p^m}-x$, and all these roots lie in $F$. So $L=F$, and $x^{p^m}-x$ must split in $F$. The roots of $x^{p^m}-x$ in $F$ form a field $K$ of order $p^m$.

## 7.2 The multiplicative group of a finite field

If $F$ is any field then the non-zero elements of $F$ form a group under multiplication. If $F$ is a finite field then it turns out that this multiplicative group is cyclic.

Let $F$ be a finite field of order $p^n$, and let $F^*$ be the multiplicative group of non-zero elements in $F$. Then $|F^*|=p^n-1$, and by Lagrange's Theorem the (multiplicative) order of every element in $F^*$ divides $p^n-1$. To show that $F^*$ is a cyclic group we need to show that $F^*$ has an element of order exactly $p^n-1$. The

key to establishing this is to note that for any positive integer $m$ there can be at most $m$ elements in $F^*$ of order dividing $m$. This is because if $a \in F^*$ has order dividing $m$ then $a$ is a root of the polynomial $x^m - 1$, and a polynomial of degree $m$ can have at most $m$ roots in the field $F$. But we can say something stronger about the number of elements of order exactly $m$. One possibility (clearly) is that there are no elements in $F^*$ of order $m$. [For example, this must be the case if $m$ does not divide $p^n - 1$.] But consider the case when $F^*$ *does* have an element $a$ of order $m$. Then there are $m$ distinct powers

$$1, a, a^2, \ldots, a^{m-1} \in F^*,$$

and all these elements have order dividing $m$. So there are at least $m$ elements in $F^*$ of order dividing $m$. But by the remarks above we know that there are at most $m$ elements in $F^*$ of order dividing $m$. This means that there are exactly $m$ elements in $F^*$ of order dividing $m$, and that these are the elements $1, a, a^2, \ldots, a^{m-1}$. So if $b \in F^*$ has order $m$ then $b = a^k$ for some $k$ with $0 < k < m$. Next, note that if $\gcd(k, m) = d$ then $a^k$ has order $m/d$, so that $a^k$ has order $m$ if and only if $\gcd(k, m) = 1$. We define $\varphi(m) = |\{k \mid 0 < k < m, \gcd(k, m) = 1\}|$, so that the number of elements in $F^*$ of order exactly $m$ is $\varphi(m)$. Putting all this together, we see that if $m$ is any positive integer then the number of elements in $F^*$ of order exactly $m$ is either 0 or $\varphi(m)$. Since the number of elements of order $m$ is certainly 0 if $m$ does not divide $p^n - 1$ we see that

$$p^n - 1 = |F^*| \leq \sum_{m|(p^n-1)} \varphi(m)$$

with equality only possible if $F^*$ has elements of order $m$ for *every* $m|(p^n - 1)$. However, if $G$ is the cyclic group of order $p^n - 1$ then $G$ has exactly $\varphi(m)$ elements of order $m$ for every $m$ dividing $p^n - 1$ and so

$$p^n - 1 = |G| = \sum_{m|(p^n-1)} \varphi(m).$$

So we must have equality in the equation

$$|F^*| \leq \sum_{m|(p^n-1)} \varphi(m),$$

and $F^*$ has elements of order $m$ for *every* $m|(p^n - 1)$. In particular, $F^*$ has elements of order $p^n - 1$ and $F^*$ is cyclic.

The usual proof that the multiplicative group of a finite field is cyclic given in the literature uses the Fundamental Theorem of Abelian groups, which (among other things) states that every finitely generated abelian group is a direct sum of cyclic subgroups. Here, we have given a proof which does not use the Fundamental Theorem.